

Rec'd PCT/PTO 22 DEC 2004

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
15 January 2004 (15.01.2004)

PCT

(10) International Publication Number
WO 2004/006520 A1

(51) International Patent Classification: H04L 12/66,
29/08

(74) Agent: FISHER ADAMS KELLY; Level 13 AMP Place,
10 Eagle Street, BRISBANE, Queensland 4001 (AU).

(21) International Application Number:
PCT/AU2003/000860

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(22) International Filing Date: 3 July 2003 (03.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data: PS 3391 4 July 2002 (04.07.2002) AU

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(72) Inventors; and

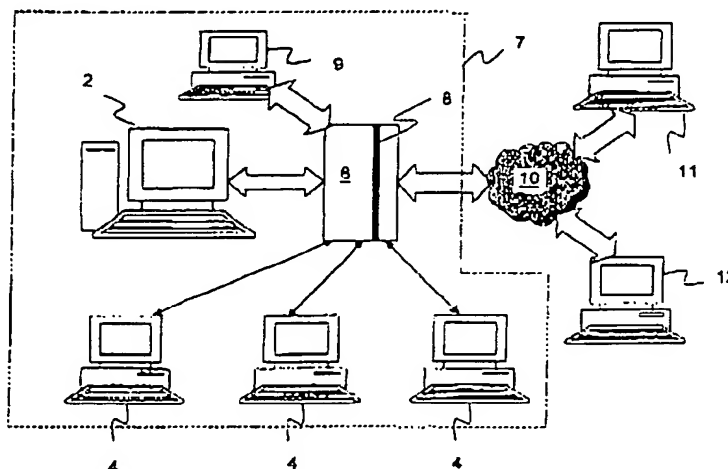
(75) Inventors/Applicants (*for US only*): SMIDT, Jeffrey, Raymond [AU/AU]; 10 Hampson Street, BURNETT HEADS, Queensland 4670 (AU). HOLLIS, Arron [AU/AU]; 10 Hampson Street, BURNETT HEADS, Queensland 4670 (AU).

Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD, SYSTEM AND APPARATUS FOR MONITORING AND CONTROLLING DATA TRANSFER IN COMMUNICATION NETWORKS



(57) Abstract: A method of monitoring and controlling data transfer between user terminals (4) coupled to a first communication network (7) and a second communication network (10) via a gateway (6) and a firewall (8) includes the user terminals (4) sending access requests to the gateway (6), the gateway (6) reading each access request, modifying access rules in the firewall (8) to permit access for each user terminal requesting access based on an authenticated IP address of each user terminal and monitoring simultaneously at the firewall (8) the transfer of data between each user terminal (4) and the second communication network (10). Bandwidth allocation to the terminals may be dynamically controlled on a global or local basis.

BEST AVAILABLE COPY

WO 2004/006520 A1

10/519263

6/PRTS

15 Rec'd PCT/PTO 22 DEC 2004

WO 2004/006520

PCT/AU2003/000860

1

METHOD, SYSTEM AND APPARATUS FOR MONITORING AND
CONTROLLING DATA TRANSFER IN COMMUNICATION NETWORKS

The invention relates to a method, system and apparatus for monitoring and controlling data transfer in communication networks. In particular, the invention relates to a method, system and gateway that enable an organization to monitor and control the data usage and online time of multiple terminals in an internal network. However, it is envisaged that the method, system and apparatus have other applications.

BACKGROUND TO THE INVENTION

There are now very few businesses, organizations, undertakings or the like that do not rely on one or more computer systems of one description or another. The computer system may be, at one end of the spectrum, a single desktop personal computer/workstation/terminal used by a small business with a single employee or, at the other end of the spectrum, the computer system may comprise tens, hundreds or thousands of terminals connected to the same system via a plurality of servers on different networks connected to one or more mainframe computers.

Irrespective of the size of the computer system access is often required to a communication network other than the one to which the terminal is connected. To access, for example, an external communication network such as the Internet, an Internet service or access provider (ISP/IAP) is required. Commonly, the ISP/IAP provides the necessary software, username(s), password(s) and the like for a monthly fee. The fee may be a flat fee, such as

WO 2004/006520

2

PCT/AU2003/000860

with a broadband connection, or may be dependent on the amount of online time and/or data transferred, e.g. uploaded and/or downloaded.

It is desirable that individual users and/or organizations are able to monitor the amount of time spent connected to another communication network and the volume of data transmitted over that connection, e.g. for reconciliation and/or security purposes.

Returning to the Internet access example, a known method for monitoring online time is employed by, for example, Internet cafés, which enables the café to bill customers according to their period of usage at preset rates, depending on, for example, the nature of their usage, e.g. gaming, browsing, LAN. One such product is known as Geto Manager developed by Advanced Com Tech Co. Ltd and details of this product are disclosed at www.swplaza.co.kr. This system comprises a plurality of user terminals networked to a management terminal (server), which may be used by members and non-members. Once users log in with an ID, a time counter commences automatically along with a fee calculator. If the user changes to another terminal, the change is automatically processed. Payment is made at the counter with a card or membership ID. In this system, the start time, account details such as pre- and post- payment details, remaining time and billing rate may be monitored by and displayed on the management terminal at, for example, the counter of the Internet café. Some of these details may also be displayed on the user's terminal. Control functions available to the management terminal include automatic locking/unlocking, rebooting and/or power switch off of individual terminals. However, this product cannot monitor the data volume being uploaded or downloaded by each terminal.

WO 2004/006520

3

PCT/AU2003/000860

Monitoring the amount of data may be carried out on individual workstations using a conventional DU meter, which shows the amount of data being uploaded and/or downloaded and the data upload/download rate. Details of a DU meter by Hagel Technologies are described at <http://www.dumeter.com>. The DU meter allows the monitoring period to be configured by the user, provides alerts when data uploads and or downloads exceed a user-specified volume in a user-specified period and provides alerts when online time exceeds a user-specified time limit. However, this facility only functions relatively accurately on an individual machine. For example, in an internal network of multiple user terminals connected to the Internet, a DU meter would register all traffic coming to the terminal on which the DU meter is installed, including traffic through the Internet gateway and crosstalk between the multiple user terminals. The DU meter is incapable of discerning the function of the data packets or their origin.

Hence, there remains a need for a system and/or method and/or apparatus that enables monitoring of data usage and time usage of any one or multiple users over multiple terminals coupled to one or more communication networks. It is also desirable that the system and/or method and/or apparatus enables analysis of data and time usage of the users/terminals and includes security measures to permit/deny access to one or more external communication networks.

DISCLOSURE OF THE INVENTION

According to one aspect, although it need not be the only or indeed the broadest aspect, the invention resides in a method of monitoring and

WO 2004/006520

PCT/AU2003/000860

4

controlling data transfer between each user terminal coupled to a first communication network and a second communication network via a gateway and a firewall, said method including the steps of:

5 sending an access request to said gateway from each said user terminal requiring access to said second communication network;

said gateway reading each said access request;

modifying at least one access rule in said firewall to permit access for each said user terminal requesting access based on an authenticated IP address of each said user terminal; and

10 monitoring simultaneously at said firewall transfer of data between each said user terminal and said second communication network.

The method may further include the step of dynamically controlling bandwidth available to each said user terminal in real time. A restricted bandwidth may be allocated on the fly to a single user terminal, a plurality of user terminals and/or one or more specified user accounts. Bandwidth may
15 be controlled for uploading and/or downloading data.

The method may further include the step of enabling and/or disabling one or more ports of access to each user terminal.

Optionally, a single machine may include the gateway and the firewall.
20 Alternatively, the firewall may be in a different machine from the gateway.

Authentication of the IP address is preferably carried out by the gateway. Authentication may be carried out using an encryption/decryption process.

The method may further include the step of controlling access of a user
25 terminal to the second communication network from a management terminal

WO 2004/006520

5

PCT/AU2003/000860

coupled to the first communication network.

The method may further include the step of monitoring a period of time a user terminal has access to the second communication network.

5 The method may further include the step of monitoring a quantity of data a user terminal uploads and/or downloads.

The method may further include the step of monitoring a cost to a user of their user terminal having access to the second communication network.

10 According to another aspect, the invention resides in a system for monitoring and controlling data transfer in communication networks, said system comprising:

one or more user terminals coupled to a first communication network;

a second communication network coupled to said first communication network via a gateway and a firewall;

15 wherein said firewall simultaneously monitors transfer of data between each said user terminal and said second communication network for each user terminal having an authenticated IP address that has access to said second communication network.

Optionally, a single machine may include the gateway and the firewall. Alternatively, the firewall may be in a different machine from the gateway.

20 Authentication of the IP address is preferably carried out by the gateway and may involve an encryption/decryption process to authenticate a remote terminal.

25 The system may further include dynamically controlling bandwidth available to each said user terminal in real time. A restricted bandwidth may be allocated on the fly to a single user terminal, a plurality of user terminals

WO 2004/006520

PCT/AU2003/000860

6

and/or one or more specified user accounts. Bandwidth may be controlled for uploading and/or downloading data.

According to a further aspect, the invention resides in a gateway for monitoring and controlling data transfer in communication networks, said gateway comprising:

a firewall for permitting access to a second communication network for each user terminal coupled to a first communication network having an authenticated IP address;

wherein said gateway monitors simultaneously at said firewall transfer of data between each said user terminal and said second communication network.

The gateway may further comprise means for dynamically controlling bandwidth allocated to each said user terminal in real time.

The gateway may further comprise means for enabling and/or disabling one or more ports of access to each user terminal.

Further aspects and features of the invention will become apparent from the following description.

BRIEF DESCRIPTION OF THE DRAWINGS

To assist in understanding the invention and to enable a person skilled in the art to put the invention into practical effect preferred embodiments of the invention will be described by way of example only with reference to the accompanying drawings, wherein:

FIG. 1 shows a schematic representation of a computer system in accordance with the present invention in which the method and apparatus of

WO 2004/006520

PCT/AU2003/000860

7

the present invention may be implemented;

FIG. 2 shows a flowchart depicting the method steps of the present invention for connecting and disconnecting a user terminal to an external communication network such as the Internet;

5 FIG. 3 shows a screenshot of part of a monitoring and control interface for monitoring terminal activity;

FIG. 4 shows a screenshot of part of the monitoring and control interface for setting pricing structures;

10 FIG. 5 shows a screenshot of part of a monitoring and control interface showing terminals defined within a network; and

FIG. 6 shows a screenshot of part of a monitoring and control interface for editing settings for a particular user terminal or user account.

DETAILED DESCRIPTION OF THE INVENTION

15 The method of the present invention may be implemented in the system of the present invention shown in FIG. 1. FIG. 1 may represent a computer system in, for example, an Internet café, a small, medium-sized or large business or other form of organization utilizing a computer system. However, the system of the present invention is not limited to the example
20 shown in FIG. 1 and the system of the present invention may apply to any two communication networks coupled by a gateway.

The system in FIG. 1 comprises one or more user terminals 4 and one or more management terminals 2 coupled to gateway terminal 6. The management terminal(s) 2 can also be considered as user terminals.

25 Together, user terminal(s) 4, management terminal(s) 2 and gateway 6 may

WO 2004/006520

PCT/AU2003/000860

8

be considered as a first communication network in the form of an internal network 7. The gateway 6 may also comprise a firewall 8 employing any known firewall technique that allows customizable rules. Alternatively, the firewall 8 may be installed in a separate machine such as terminal 9 coupled to the gateway 6. The Internal network 7 communicates through gateway 6 with one or more second communication networks in the form of one or more external networks 10. Such external networks 10 are external to the internal network 7 and may be the Internet, wide area networks, or secured sections of any network based on the Internet Protocol TCP/IP. Persons skilled in the art will appreciate that the gateway 6 may also be associated with a router located between the gateway and the external network 10 and a switch located between the gateway 6 and the terminals 2, 4 to direct information in and out of the gateway 6.

As alternatives to the system shown in FIG. 1, the system of the present invention may comprise a gateway 6 and firewall 8 between two public networks or between two private networks and therefore the system and method of the present invention are not limited to the Internal and external networks shown in FIG. 1. It will therefore be appreciated that the internal and external networks referred to in the following example may be substituted for public or private networks or a combination thereof.

The method of the present invention is described with further reference to the flowchart in FIG. 2 and the screenshots in FIGS. 3-6. At step 20, the levels of logging, such as gaming or browsing or other functions, are set, as well as levels of pricing, if appropriate. Examples are shown in FIG. 4. Logging of activities is carried out by the firewall 8 and may be carried out on

WO 2004/006520

9

PCT/AU2003/000860

a per data quantity basis, e.g. per Mb, and/or on a per unit time basis, e.g. per second, per minute or other time period. For example, time may be logged at a preset cost per unit time. There may also, or alternatively, be a data upload and/or download limit, which, if exceeded, may incur a further charge in addition to, or as an alternative to, the time spent by the user at the terminal. Alternatively, the cost may be charged on whichever is greater based on time or uploads/downloads. It will be appreciated that there are many permutations by which logging may be carried out and that the present invention is not limited to any particular permutation.

At step 22, a user logs into a user terminal 4, such as a customer in an Internet café or an employee in a business. There may be any number of pricing levels, classes or timing categories or the like, which will depend on the particular user and/or the application, e.g. large organization, Internet café.

With reference to step 24 in FIG. 2, if a user does not require access to an external network 10, such as the Internet, the monitoring and control method of the present invention does not come into operation and once the user has logged in they are enabled for their own network, i.e. not an external network. However, if a user does require, for example, Internet access, a request for access in the form of a data packet containing the Internet protocol (IP) address of the user's terminal may be added to an access queue in the gateway 6, as represented by step 26. However, operating speeds are sufficiently high that queuing will usually be unnecessary and the requests will be processed substantially instantaneously.

When the IP address is read by the gateway 6, the gateway generates

WO 2004/006520

10

PCT/AU2003/000860

a rule to instruct the firewall 8 to permit access to that IP address. The firewall 8 follows the generated rule and permits external network access to that IP address, as represented by step 28, providing the IP address has been authenticated via a username and password at the gateway 6 for access to an external network 10. Access to an external network is granted to the user and the terminal by amending one or more rules in a list of rules followed by the firewall. The rules enable the firewall to permit or deny network access to specific IP addresses. Rules may be added or removed. Alternatively, existing rules may be changed/updated to permit or deny external network access.

FIG 3 shows a monitoring and control interface available on the management terminal 2, which shows those terminals that are and are not in use. The identity of each terminal and the section to which it belongs within its network are displayed in addition to the user of that terminal. The usage time, the data volume downloaded in Mbs and the associated cost are displayed.

When external network access is enabled for a particular terminal, specific access port numbers of that terminal may be enabled/disabled to permit/forbid respectively particular activities, such as gaming and/or browsing and/or other activities being performed from the terminal. The particular ports of access to a terminal that are enabled/disabled may depend on the particular user and/or on the particular terminal. Enabling/disabling of the ports is controlled by the rules provided to and followed by the firewall 8. The rules may be set up, for example, when a user account is created. A default option may be that all ports are activated to permit all activities at a terminal,

WO 2004/006520

11

PCT/AU2003/000860

as shown in the top left hand corner of FIG. 6.

FIG. 6 also shows that exceptions may be specified to the settings of "Allow All Ports" or "Block All Ports". For example, FIG. 6 shows that all ports are allowed for the Arron(1) account for all activities except SSH (Secure Shell) because the SSH box is checked in the Exceptions section. SSH allows the user to log into another terminal over the external communications network or another network to execute commands in the remote terminal and to move files from one machine to another. One or more of the exceptions boxes may be checked to permit or forbid the activity represented by the box, depending on whether the "Block" or "Allow" box for the ports is checked respectively. Another example might be that HTML is permitted, but no other type of data transfer.

With further reference to FIG. 6, the bandwidth, or data transfer rate, allocated to one or more terminals may also be dynamically controlled on the fly by the system and method of the present invention. Bandwidth may be controlled globally or locally and in real time without interfering with the network to which the terminal is coupled or otherwise interrupting communications.

Global bandwidth settings affect every terminal connected to the gateway 6 and any changes to the settings are effected globally. For example, if port 80, which is generally used for Internet connection, is blocked globally, each terminal connected to the gateway 6 will not be able to access the Internet via port 80. In another example, if a bandwidth of, for example, 2 Mb/s is allocated for web access, all terminals connected to the Internet will share the 2 Mb/s bandwidth.

WO 2004/006520

12

PCT/AU2003/000860

Local bandwidth settings only affect one or more specified terminals or user accounts. For example, a specified bandwidth may be allocated to a particular terminal, such as the management terminal 2. The advantage of allocating a specified bandwidth to a user account on the other hand, as shown in FIG. 6, is that the user will be able to use their allocated specified bandwidth irrespective of the terminal that they are logged into. In the example shown in FIG. 6, no bandwidth restriction is set for uploads, but the download bandwidth is limited to 10Mb/s for the Arron(1) user account.

A further feature of the bandwidth control is that exceptions may be specified to the bandwidth restrictions as shown in FIG. 6. For example, in FIG. 6, as with the port limitation example described above, the SSH (Secure Shell) box is checked. In this example, the 10Mbit/s download limit therefore will not apply to SSH download operations for this user account. The other, non-exhaustive examples of bandwidth restriction exemptions shown in FIG. 6 are for protocols/applications/networks that will be familiar to persons skilled in the art.

The dynamic bandwidth allocation feature of the present invention allows bandwidth to be allocated to users, terminals and/or groups thereof as required. For example, organizations such as schools and other educational institutions usually only have a limited bandwidth allocation and the present invention allows the bandwidth or a part thereof to be allocated to one or more terminals for, e.g. a media streaming event. The bandwidth allocation may be for a prescribed time period after which, the bandwidth may be reallocated, e.g. to one or more different terminals.

Bandwidth allocation may be on a priority basis whereby users and/or

WO 2004/006520

13

PCT/AU2003/000860

specific terminals are allocated a priority, e.g. a number 1 to 5. If two or more terminals and/or users are competing for bandwidth, the terminal and/or user with the highest priority is allocated the bandwidth.

Another scenario could be a medical environment such as a hospital, where bandwidth requirements can vary rapidly. For example, data files containing medical images such as X-rays, MRI and/or CAT scans, which can be large, often need to be transferred between networks within and between medical establishments. Bandwidth may be allocated dynamically to facilitate the transfer of such files. This enables the file(s) to be transferred rapidly, which is often necessary in emergency situations and prevents the computer system of the medical establishment from grinding to a halt while the file(s) are transferred.

Once network access to a specific IP address is permitted, logging of that terminal's activity is commenced by the firewall 8, as represented by step 30 in FIG. 2. The type of data that will be logged includes start time, current session time, monetary cost incurred this session, user/customer limit(s) (in terms of time, expenditure and/or data volume), account type (e.g. debit or credit) and/or account status. Firewall 8 records such data for each particular IP address connected to the external network 10. This data can then be requested by the gateway 6 and displayed, as described hereinafter.

Once a user has logged in and gained access to the external network 10, it is not possible for the user to revert back to a previous screen prior to log in, e.g. by clicking on the "back" button, in an attempt to circumvent the monitoring and logging of their session by the method of the present invention.

WO 2004/006520

14

PCT/AU2003/000860

Once a user has completed their session, e.g. at the end of a working day in the case of a business employee, the user logs out of the terminal, as shown at step 32. Alternatively, the gateway 6 and firewall 8 may cause the user to be logged out and disconnected from the external network 10 if, for example, the user's preset time limit has expired. This may be set such that a user's session is terminated automatically. Alternatively, an operator of the management terminal 2 may effect session termination by initiating a disconnection request. In this way the operator can inform the user prior to session termination to avoid a user losing any important data. A user may only terminate their own session and not the session of another user unless this is done via a management terminal 2. In this case it should be an authorized staff member e.g. in the case of an organization or Internet café, who will have the required username and password to use a management terminal 2.

Once logging out has been initiated, either by the user or by the request from a management terminal 2, a request for disconnection from the external network in the form of a data packet containing the IP address of the terminal to be disconnected may be added to a disconnection queue in the gateway 6, as represented by step 34. Once again however, queuing will usually be unnecessary and the request for disconnection will be processed substantially instantaneously.

When the IP address of the disconnection request is read, the rule(s) that permits access for that particular IP address is/are removed/amended from/in the firewall 8 and the firewall disables access to the external network for that IP address, as represented by step 36 in FIG 2.

WO 2004/006520

15

PCT/AU2003/000860

Once the firewall 8 has processed a queued connection request or disconnection request, that request is cleared from the queue to prevent processing of the request being duplicated in error.

A session history is maintained by the gateway 6 based on the data logs created by the firewall 8, as represented by step 38. Each session history contains relevant information for that particular user terminal and/or that particular user. The relevant information may include the terminal and user ID, log on and log off times, session duration, billing rate, data volume consumption/upload/download, data upload/download limit(s), session cost, payment method, account status, URLs visited and the time spent visiting each URL and other such information. The type of information contained in the session history may be determined by the gateway 6 and the firewall 8 on a per user and/or per terminal basis as required. This information may be compared to billing information that is supplied by the service provider.

The activity of users can be monitored at a management terminal 2 by virtue of the monitoring and control interface in the form of, for example, a table displaying which terminals are and which terminals are not in use and the relevant data associated with that terminal usage, as shown in FIGS. 3-6 and described herein. However, the present invention is not limited to the monitoring and control interface being accessible just on a single management terminal. The interface may be accessed on any terminal in the system that has been given access to management controls. FIG. 5 shows a table displaying details of the currently defined terminals (machines), which includes the identity of the machine, the section to which it belongs, its IP address, a Media Access Control (MAC) address and whether or not the

WO 2004/006520

16

PCT/AU2003/000860

terminal is active.

If, for example, there is a problem with the gateway 6 or there is power loss and external network access is lost to all terminals, the present invention enables a management terminal 2 to re-connect each terminal with the external network with which it was connected before connection was lost (providing connection to the relevant external network is possible). The firewall 8 accepts a request to restore the external network connection from a management terminal 2. The firewall restores the connections to their previous status since the IP addresses of the terminals have previously been verified by the gateway 6 and enabled by the firewall 8. Each individual user does not need to request access to the external network again for that session.

The monitoring and control interface, which is accessible on whichever terminal(s) is/are operating as a management terminal, offers the operator other control features including, but not limited to, a general settings feature, back up options, accounts, access settings and display/edit of staff access codes.

The general settings feature provides control over the firewall 8 and/or the gateway 6 and enables the monitoring and control method to operate as a passive booking system. This enables time slots to be allocated to particular users and/or particular terminals. Hence, if a particular time slot or terminal has been reserved and a different user attempts to log on to the reserved terminal during the reserved time slot, an alert will be activated to the user and/or the management terminal 2. The operator of the management terminal may be given the option to override the time slot and/or terminal reservation.

WO 2004/006520

17

PCT/AU2003/000860

Varying levels of security access may be set for different staff and managers and the like according to their permissions/seniority/security clearance or the like. For example, staff may have their own log in screens to enable monitoring and, to an extent, control of their own terminal usage by the method of the present invention. Staff may be permitted to enable/disable external network access, but may not be able to, for example, view accounting details, which could be reserved for managerial access.

The back up options feature may, for example, provide for one or more alternative server addresses, identifications and/or passwords in the event of failure of those normally employed.

The present invention may be used for a "walled garden" in, for example, a motel or educational establishment. Accessing sites within the controlled browsing environment may be free, but accessing sites outside the walled garden may incur a fee. The firewall 8 will monitor all access and log charges accordingly.

The method of the present invention enables the data related to staff/user access described above to be monitored and access to one or more networks external to the terminal being monitored to be controlled remotely on a per user, per machine basis and/or on a per user over multiple machines basis. This includes not only time monitoring, but also data volume usage monitoring because the traffic for each IP address, i.e. terminal, is being logged by the firewall 8 and monitored at the gateway 6.

The system employing the method is also resistant to security breaches of the system because the method monitors all traffic through the gateway 6 and firewall 8. Any attempted unauthorized access from an

WO 2004/006520

18

PCT/AU2003/000860

external terminal 11 will require the IP address associated with the external terminal 11 to be identified. The firewall 8 creates logs for each terminal based on the IP address of the terminal and the user ID entered by the user of that terminal. The rules of the firewall will not have been altered/added to in order to permit access/traffic flow between the external terminal 11 and the internal network 7 via the firewall 8 and the gateway 6. Therefore, the external terminal should not gain access to the internal network 7. Furthermore, the method of the present invention restarts the firewall periodically after a short time period, e.g. 2 seconds, has elapsed. Therefore, in the event that the unauthorized external terminal 11 somehow disables the firewall 8, it will be restarted within a short time to once again automatically deny access to the unauthorized external terminal 11. The restarted firewall 8 will not include an authenticated IP address of the external terminal 11. Any activity of the unauthorized external terminal will therefore be identified because their activities will be logged and the unauthorized external terminal 11 will be identified by an alert on the management terminal(s). Similarly, any unauthorized terminals may not be connected to the network since they will have an unrecognized IP address. Therefore, a member of staff e.g. in a business, or a member of the public using an Internet café, cannot connect their own machine to the network.

The method, system and apparatus of the present invention also allows for permitting access to the internal network 7 by one or more authorized remote terminals 12 that are not part of the internal network 7 shown in FIG. 1. Authorization may be conducted via, for example, email and/or using security keys. For example, the gateway 6 may comprise a public encryption

WO 2004/006520

19

PCT/AU2003/000860

key supplied by a user of a remote terminal 12. The user of the remote terminal 12 will have a private encryption/decryption key. When the remote terminal requests access to the Internal network 7, the gateway 6 will send a message encrypted with the public key to the remote terminal. The remote terminal 12 decrypts the encrypted message and returns the decrypted message to the gateway 6. The gateway compares the received decrypted message with the original unencrypted message. If they are the same the identity of the remote terminal has been successfully authenticated and the gateway 6 grants access to the internal network 7 to the remote terminal 12.

The gateway then acquires the IP address of the remote terminal 12 from the access data packets and the gateway can monitor the activity of the remote terminal 12 as described for terminals 4 herein. If the original and decrypted messages differ, access is denied since the identity of the remote terminal has not been verified. A user ID and password may be used in conjunction with the security keys. This method of permitting access to remote terminals applies to both permanent and temporary external IP addresses. The activities of the remote terminals will also be displayed on the management terminal(s).

The method of the present invention operates on any known operating system that has HTML capability on the staff/user terminals, although the Unix/Linux operating system is preferred. Where the server side needs more than HTML capabilities, it has to be configured to the appropriate operating system's gateway/firewall structures.

The present invention works with wireless networks, network printers and/or any program or device that works over TCP/IP protocol. The method

WO 2004/006520

20

PCT/AU2003/000860

also fully supports Dynamic Host Controller Protocol (DHCP) and may be employed on larger networks requiring subnets and a plurality of gateways. The method and gateway may be installed via a conventional bootable flash memory familiar to persons skilled in the art. The present invention does not
5 require specialist software to be installed on each terminal that is to be monitored and reconfiguration of the network is not required. Software only needs to be installed on the gateway machine and the gateway will search for machines connected to the network.

Another advantage of the present invention is that it does not cache
10 any data, e.g. data relating to web pages, which is performed by some of the prior art systems. Hence, the present invention enables users to, for example, view current web pages and not potentially out of date web pages that have been cached.

Throughout the specification the aim has been to describe the
15 invention without limiting the invention to any one embodiment or specific collection of features. Persons skilled in the relevant art may realize variations from the specific embodiments that will nonetheless fall within the scope of the invention.

WO 2004/006520

21

PCT/AU2003/000860

CLAIMS

1. A method of monitoring and controlling data transfer between each user terminal coupled to a first communication network and a second communication network via a gateway and a firewall, said method including the steps of:

5 sending an access request to said gateway from each said user terminal requiring access to said second communication network;

said gateway reading each said access request;

10 modifying at least one access rule in said firewall to permit access for each said user terminal requesting access based on an authenticated IP address of each said user terminal requesting access; and

monitoring simultaneously at said firewall the transfer of data between each said user terminal and said second communication network.

15 2. The method of claim 1 further including the step of dynamically controlling bandwidth available to one or more of said user terminals in real time.

20 3. The method of claim 2, wherein a restricted bandwidth is allocated to a single user terminal.

4. The method of claim 2, wherein a restricted bandwidth is shared between a plurality of user terminals.

WO 2004/006520

22

PCT/AU2003/000860

5. The method of claim 2, wherein bandwidth is restricted for uploading data and/or downloading data.

6. The method of claim 2, wherein a restricted bandwidth is allocated to one or more terminals for a prescribed time period.

7. The method of claim 2, wherein a restricted bandwidth is allocated to one or more terminals on the basis of a priority status allocated to the one or more terminals or a user account.

8. The method of claim 1, wherein the IP address of a user terminal is authenticated on the basis that the user terminal has previously been authenticated by the gateway using an encryption/decryption process.

9. The method of claim 1 further including the step of enabling and/or disabling one or more ports of access to a user terminal.

10. The method of claim 1 further including the step of controlling access of a user terminal to the second communication network from a management terminal coupled to the first communication network.

11. The method of claim 1 further including the step of monitoring a period of time a user terminal has access to the second communication network.

WO 2004/006520

23

PCT/AU2003/000860

12. The method of claim 1 further including the step of monitoring a quantity of data a user terminal uploads and/or downloads.

13. The method of claim 1 further including the step of monitoring a cost to a user of their user terminal having access to the second communication network.

14. A system for monitoring and controlling data transfer in communication networks, said system comprising:

one or more user terminals coupled to a first communication network;
a second communication network coupled to said first communication network via a gateway and a firewall;
wherein said firewall simultaneously monitors transfer of data between each said user terminal and said second communication network for each user terminal having an authenticated IP address that has access to said second communication network.

15. The system of claim 14, wherein a single machine comprises both the gateway and the firewall.

16. The system of claim 14, wherein the firewall is in a different machine from the gateway.

17. The system of claim 14, wherein authentication of the IP address is carried out by the gateway.

WO 2004/006520

24

PCT/AU2003/000860

18. The system of claim 17, wherein authentication employs an encryption/decryption process to authenticate a remote terminal.

19. The system of claim 14, wherein bandwidth available to the one or more user terminals is dynamically controlled in real time.

20. The system of claim 14, wherein a restricted bandwidth is allocated to a single user terminal.

21. The system of claim 14, wherein a restricted bandwidth is shared between a plurality of user terminals.

22. The system of claim 14, wherein a restricted bandwidth is allocated to a user account.

23. The system of claim 14, wherein bandwidth is restricted for uploading data and/or downloading data.

24. A gateway for monitoring and controlling data transfer in communication networks, said gateway comprising:
a firewall for permitting access to a second communication network for each user terminal coupled to a first communication network having an authenticated IP address;

WO 2004/006520

25

PCT/AU2003/000860

wherein said gateway monitors simultaneously at said firewall transfer of data between each said user terminal and said second communication network.

5 25. The gateway of claim 24 further comprising means for dynamically controlling bandwidth allocated in real time to each said user terminal.

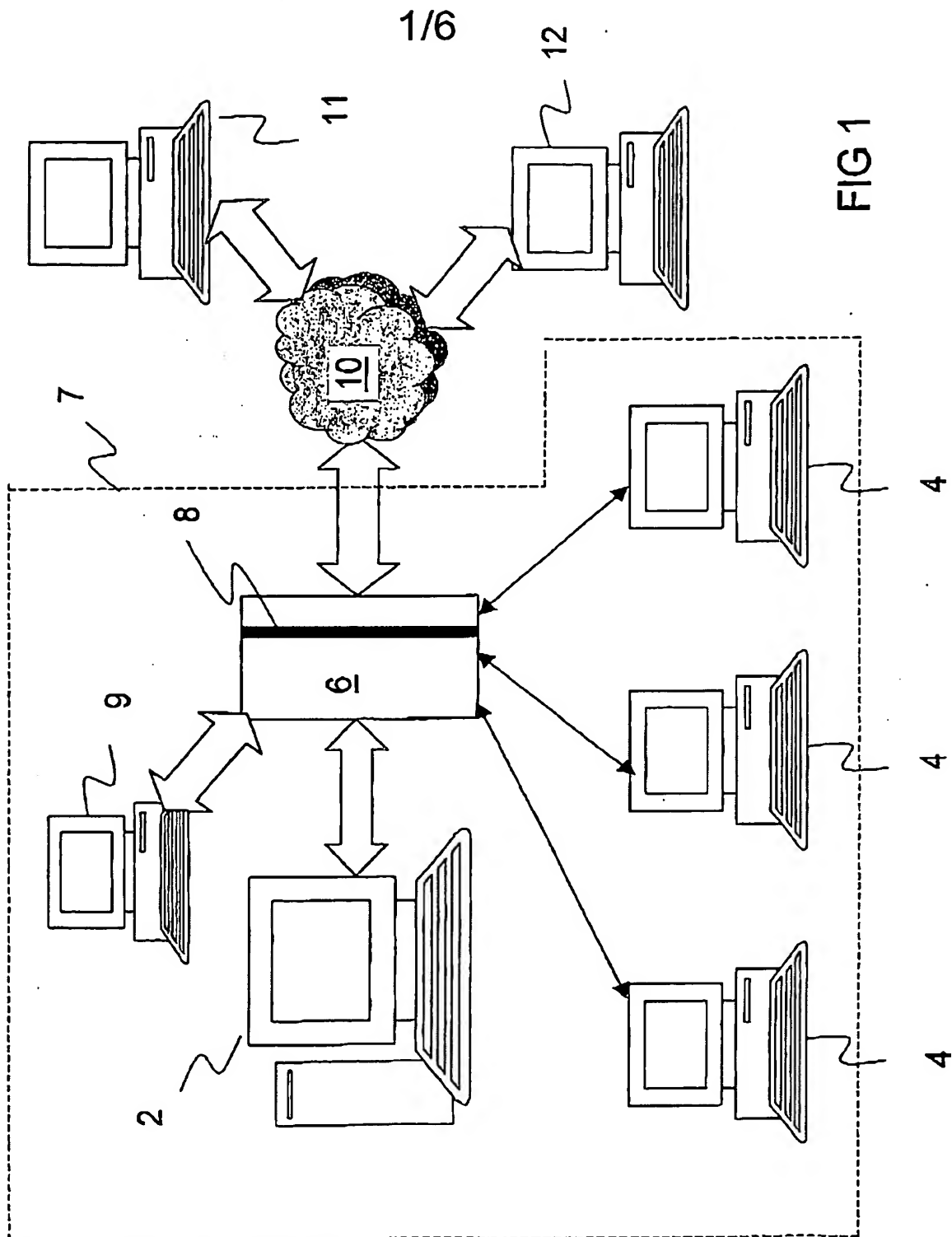
26. The gateway of claim 24 further comprising means for enabling and/or disabling one or more ports of access to each user terminal.

10

10/519263

WO 2004/006520

PCT/AU2003/000860



10/519263

WO 2004/006520

PCT/AU2003/000860

2/6

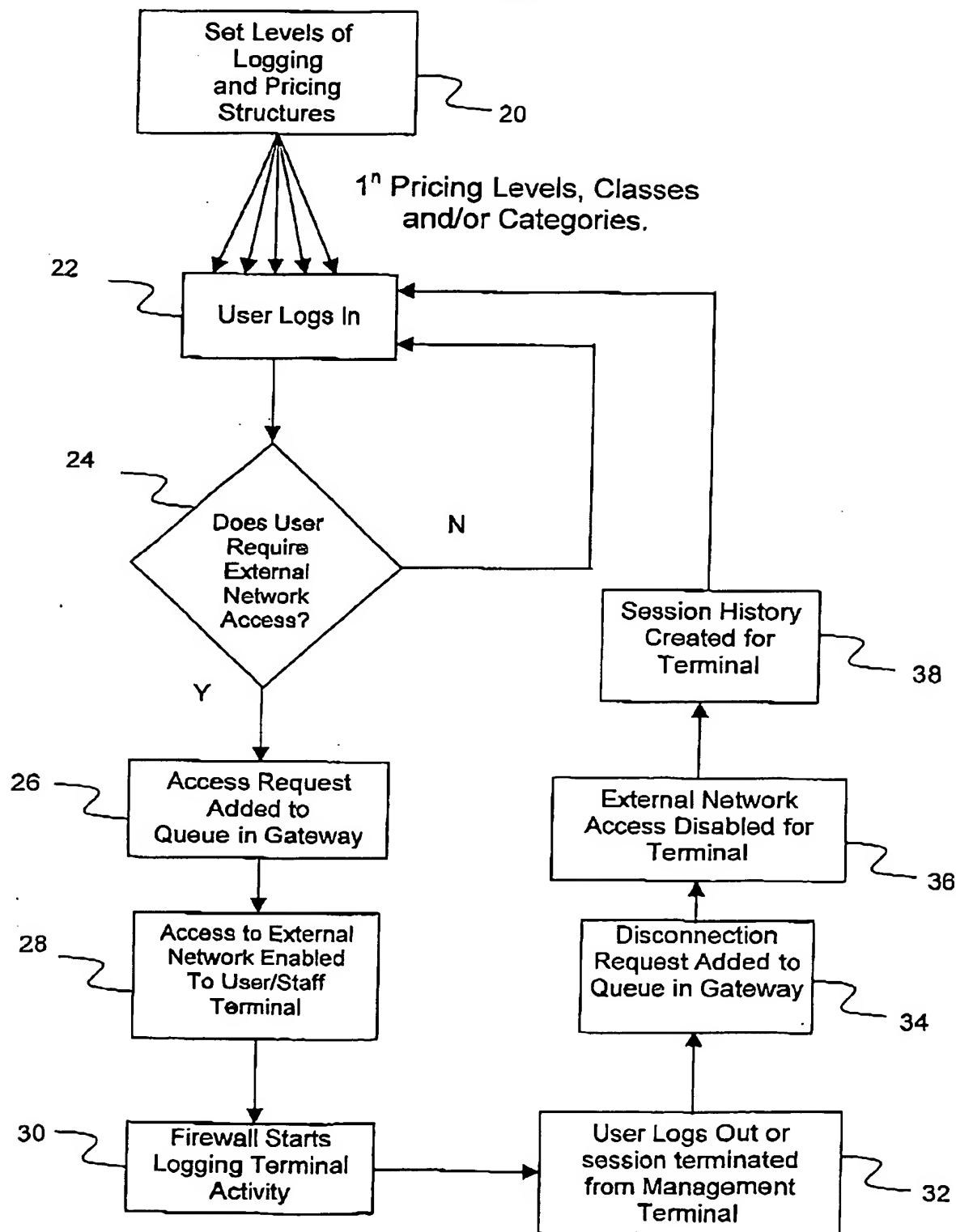


FIG 2

10/519263

WO 2004/006520

PCT/AU2003/000860

3/6

C:\WINDOWS\Local Settings\Temporary Internet Files\Content.IE5\EJC1U50X\management_main(1).htm - Telstra Dig Pond ...

User Name	Machine	Section	Mega/Min (Greatest)	Total Charge	
Arcon	Gaming 2	Game Machines	11 Minutes 59 Seconds / 10,195,316 meg	\$0.39	History
Andrew	Gaming 3	Game Machines	8 Minutes 10 Seconds / 8,372,777 meg	\$0.27	History
Kim	Gaming 4	Game Machines	11 Minutes 21 Seconds / 7,783,572 meg	\$0.38	History
Andy	Gaming 5	Game Machines	10 Minutes 33 Seconds / 8,802,883 meg	\$0.36	History
Unknown	Chat Entry	Staff Machines	20 Hours 4 Minutes / 20,005,2 meg	\$41.39	History
Jill	Chat	Staff Machines	1 Hour 57 Minutes / 1,914,444 meg	\$17.9	History
Paul Walsman	Staff	Staff Machines	4 Hours 55 Minutes / 4,169,79 meg	\$21.8	History

Display All Online Terminals Gamer's Valhalla - Activity Monitor Display Online Terminals by Group

User Name	Machine	Section	Mega/Min (Greatest)	Total Charge	
Default	Gaming 7	Game Machines	0 Seconds / 0 meg	\$0	History
Default	Gaming 8	Game Machines	0 Seconds / 0 meg	\$0	History
Default	Gaming 9	Game Machines	0 Seconds / 0 meg	\$0	History
Default	Gaming 10	Game Machines	0 Seconds / 0 meg	\$0	History
Default	Gaming 11	Game Machines	0 Seconds / 0 meg	\$0	History
Default	Gaming 12	Game Machines	0 Seconds / 0 meg	\$0	History
Renee	Gaming 1	Game Machines	4 Minutes 55 Seconds / 0 meg	\$0.16	History

Start | Stop | Refresh | Print | Close | Help | ...

FIG 3

201519263

WO 2004/006520

PCT/AU2003/000860

4/6

Screen Shot 4 - Telstra Big Pond Home Internet Explorer
 http://management.p-concept.com.au - microsoft internet explorer

Tools Help

Refresh Home Search Favorites History Menu Print Edit

Calculate Costing Method Downloads Download

Save Which server space C...

Section Pricelevel

Cafe Machine 1 Save

Staff Machine 3 Save

Cafe Machine 2 Save

Hardware 1 Save

Price Level

	Par	Par	
	Max	Hour	
1 Default	0.3	12	Save
2 For Cafe Machines	0.3	4	Save
3 Staff - Private Usage	0.3	35	Save
Add new Price Level			

Return to Main page

1600 1700 1800 1900 2000 2100 2200 2300 2400 2500 2600 2700 2800 2900 3000 3100 3200 3300 3400 3500 3600 3700 3800 3900 4000 4100 4200 4300 4400 4500 4600 4700 4800 4900 5000 5100 5200 5300 5400 5500 5600 5700 5800 5900 6000 6100 6200 6300 6400 6500 6600 6700 6800 6900 7000 7100 7200 7300 7400 7500 7600 7700 7800 7900 8000 8100 8200 8300 8400 8500 8600 8700 8800 8900 9000 9100 9200 9300 9400 9500 9600 9700 9800 9900 10000 10100 10200 10300 10400 10500 10600 10700 10800 10900 11000 11100 11200 11300 11400 11500 11600 11700 11800 11900 12000 12100 12200 12300 12400 12500 12600 12700 12800 12900 13000 13100 13200 13300 13400 13500 13600 13700 13800 13900 14000 14100 14200 14300 14400 14500 14600 14700 14800 14900 15000 15100 15200 15300 15400 15500 15600 15700 15800 15900 16000 16100 16200 16300 16400 16500 16600 16700 16800 16900 17000 17100 17200 17300 17400 17500 17600 17700 17800 17900 18000 18100 18200 18300 18400 18500 18600 18700 18800 18900 19000 19100 19200 19300 19400 19500 19600 19700 19800 19900 20000 20100 20200 20300 20400 20500 20600 20700 20800 20900 21000 21100 21200 21300 21400 21500 21600 21700 21800 21900 22000 22100 22200 22300 22400 22500 22600 22700 22800 22900 23000 23100 23200 23300 23400 23500 23600 23700 23800 23900 24000 24100 24200 24300 24400 24500 24600 24700 24800 24900 25000 25100 25200 25300 25400 25500 25600 25700 25800 25900 26000 26100 26200 26300 26400 26500 26600 26700 26800 26900 27000 27100 27200 27300 27400 27500 27600 27700 27800 27900 28000 28100 28200 28300 28400 28500 28600 28700 28800 28900 29000 29100 29200 29300 29400 29500 29600 29700 29800 29900 30000 30100 30200 30300 30400 30500 30600 30700 30800 30900 31000 31100 31200 31300 31400 31500 31600 31700 31800 31900 32000 32100 32200 32300 32400 32500 32600 32700 32800 32900 33000 33100 33200 33300 33400 33500 33600 33700 33800 33900 34000 34100 34200 34300 34400 34500 34600 34700 34800 34900 35000 35100 35200 35300 35400 35500 35600 35700 35800 35900 36000 36100 36200 36300 36400 36500 36600 36700 36800 36900 37000 37100 37200 37300 37400 37500 37600 37700 37800 37900 38000 38100 38200 38300 38400 38500 38600 38700 38800 38900 39000 39100 39200 39300 39400 39500 39600 39700 39800 39900 40000 40100 40200 40300 40400 40500 40600 40700 40800 40900 41000 41100 41200 41300 41400 41500 41600 41700 41800 41900 42000 42100 42200 42300 42400 42500 42600 42700 42800 42900 43000 43100 43200 43300 43400 43500 43600 43700 43800 43900 44000 44100 44200 44300 44400 44500 44600 44700 44800 44900 45000 45100 45200 45300 45400 45500 45600 45700 45800 45900 46000 46100 46200 46300 46400 46500 46600 46700 46800 46900 47000 47100 47200 47300 47400 47500 47600 47700 47800 47900 48000 48100 48200 48300 48400 48500 48600 48700 48800 48900 49000 49100 49200 49300 49400 49500 49600 49700 49800 49900 50000 50100 50200 50300 50400 50500 50600 50700 50800 50900 51000 51100 51200 51300 51400 51500 51600 51700 51800 51900 52000 52100 52200 52300 52400 52500 52600 52700 52800 52900 53000 53100 53200 53300 53400 53500 53600 53700 53800 53900 54000 54100 54200 54300 54400 54500 54600 54700 54800 54900 55000 55100 55200 55300 55400 55500 55600 55700 55800 55900 56000 56100 56200 56300 56400 56500 56600 56700 56800 56900 57000 57100 57200 57300 57400 57500 57600 57700 57800 57900 58000 58100 58200 58300 58400 58500 58600 58700 58800 58900 59000 59100 59200 59300 59400 59500 59600 59700 59800 59900 60000 60100 60200 60300 60400 60500 60600 60700 60800 60900 61000 61100 61200 61300 61400 61500 61600 61700 61800 61900 62000 62100 62200 62300 62400 62500 62600 62700 62800 62900 63000 63100 63200 63300 63400 63500 63600 63700 63800 63900 64000 64100 64200 64300 64400 64500 64600 64700 64800 64900 65000 65100 65200 65300 65400 65500 65600 65700 65800 65900 66000 66100 66200 66300 66400 66500 66600 66700 66800 66900 67000 67100 67200 67300 67400 67500 67600 67700 67800 67900 68000 68100 68200 68300 68400 68500 68600 68700 68800 68900 69000 69100 69200 69300 69400 69500 69600 69700 69800 69900 70000 70100 70200 70300 70400 70500 70600 70700 70800 70900 71000 71100 71200 71300 71400 71500 71600 71700 71800 71900 72000 72100 72200 72300 72400 72500 72600 72700 72800 72900 73000 73100 73200 73300 73400 73500 73600 73700 73800 73900 74000 74100 74200 74300 74400 74500 74600 74700 74800 74900 75000 75100 75200 75300 75400 75500 75600 75700 75800 75900 76000 76100 76200 76300 76400 76500 76600 76700 76800 76900 77000 77100 77200 77300 77400 77500 77600 77700 77800 77900 78000 78100 78200 78300 78400 78500 78600 78700 78800 78900 79000 79100 79200 79300 79400 79500 79600 79700 79800 79900 80000 80100 80200 80300 80400 80500 80600 80700 80800 80900 81000 81100 81200 81300 81400 81500 81600 81700 81800 81900 82000 82100 82200 82300 82400 82500 82600 82700 82800 82900 83000 83100 83200 83300 83400 83500 83600 83700 83800 83900 84000 84100 84200 84300 84400 84500 84600 84700 84800 84900 85000 85100 85200 85300 85400 85500 85600 85700 85800 85900 86000 86100 86200 86300 86400 86500 86600 86700 86800 86900 87000 87100 87200 87300 87400 87500 87600 87700 87800 87900 88000 88100 88200 88300 88400 88500 88600 88700 88800 88900 89000 89100 89200 89300 89400 89500 89600 89700 89800 89900 90000 90100 90200 90300 90400 90500 90600 90700 90800 90900 91000 91100 91200 91300 91400 91500 91600 91700 91800 91900 92000 92100 92200 92300 92400 92500 92600 92700 92800 92900 93000 93100 93200 93300 93400 93500 93600 93700 93800 93900 94000 94100 94200 94300 94400 94500 94600 94700 94800 94900 95000 95100 95200 95300 95400 95500 95600 95700 95800 95900 96000 96100 96200 96300 96400 96500 96600 96700 96800 96900 97000 97100 97200 97300 97400 97500 97600 97700 97800 97900 98000 98100 98200 98300 98400 98500 98600 98700 98800 98900 99000 99100 99200 99300 99400 99500 99600 99700 99800 99900 100000 100100 100200 100300 100400 100500 100600 100700 100800 100900 101000 101100 101200 101300 101400 101500 101600 101700 101800 101900 102000 102100 102200 102300 102400 102500 102600 102700 102800 102900 103000 103100 103200 103300 103400 103500 103600 103700 103800 103900 104000 104100 104200 104300 104400 104500 104600 104700 104800 104900 105000 105100 105200 105300 105400 105500 105600 105700 105800 105900 106000 106100 106200 106300 106400 106500 106600 106700 106800 106900 107000 107100 107200 107300 107400 107500 107600 107700 107800 107900 108000 108100 108200 108300 108400 108500 108600 108700 108800 108900 109000 109100 109200 109300 109400 109500 109600 109700 109800 109900 110000 110100 110200 110300 110400 110500 110600 110700 110800 110900 111000 111100 111200 111300 111400 111500 111600 111700 111800 111900 112000 112100 112200 112300 112400 112500 112600 112700 112800 112900 113000 113100 113200 113300 113400 113500 113600 113700 113800 113900 114000 114100 114200 114300 114400 114500 114600 114700 114800 114900 115000 115100 115200 115300 115400 115500 115600 115700 115800 115900 116000 116100 116200 116300 116400 116500 116600 116700 116800 116900 117000 117100 117200 117300 117400 117500 117600 117700 117800 117900 118000 118100 118200 118300 118400 118500 118600 118700 118800 118900 119000 119100 119200 119300 119400 119500 119600 119700 119800 119900 120000 120100 120200 120300 120400 120500 120600 120700 120800 120900 121000 121100 121200 121300 121400 121500 121600 121700 121800 121900 122000 122100 122200 122300 122400 122500 122600 122700 122800 122900 123000 123100 123200 123300 123400 123500 123600 123700 123800 123900 124000 124100 124200 124300 124400 124500 124600 124700 124800 124900 125000 125100 125200 125300 125400 125500 125600 125700 125800 125900 126000 126100 126200 126300 126400 126500 126600 126700 126800 126900 127000 127100 127200 127300 127400 127500 127600 127700 127800 127900 128000 128100 128200 128300 128400 128500 128600 128700 128800 128900 129000 129100 129200 129300 129400 129500 129600 129700 129800 129900 130000 130100 130200 130300 130400 130500 130600 130700 130800 130900 131000 131100 131200 131300 131400 131500 131600 131700 131800 131900 132000 132100 132200 132300 132400 132500 132600 132700 132800 132900 133000 133100 133200 133300 133400 133500 133600 133700 133800 133900 134000 134100 134200 134300 134400 134500 134600 134700 134800 134900 135000 135100 135200 135300 135400 135500 135600 135700 135800 135900 136000 136100 136200 136300 136400 136500 136600 136700 136800 136900 137000 137100 137200 137300 137400 137500 137600 137700 137800 137900 138000 138100 138200 138300 138400 138500 138600 138700 138800 138900 139000 139100 139200 139300 139400 139500 139600 139700 139800 139900 140000 140100 140200 140300 140400 140500 140600 140700 140800 140900 141000 141100 141200 141300 141400 141500 141600 141700 141800 141900 142000 142100 142200 142300 142400 142500 142600 142700 142800 142900 143000 143100 143200 143300 143400 143500 143600 143700 143800 143900 144000 144100 144200 144300 144400 144500 144600 144700 144800 144900 145000 145100 145200 145300 145400 145500 145600 145700 145800 145900 146000 146100 146200 146300 146400 146500 146600 146700 146800 146900 147000 147100 147200 147300 147400 147500 147600 147700 147800 147900 148000 148100 148200 148300 148400 148500 148600 148700 148800 148900 149000 149100 149200 149300 149400 149500 149600 149700 149800 149900 150000 150100 150200 150300 150400 150500 150600 150700 150800 150900 151000 151100 151200 151300 151400 151500 151600 151700 151800 151900 152000 152100 152200 152300 152400 152500 152600 152700 152800 152900 153000 153100 153200 153300 153400 153500 153600 153700 153800 153900 154000 154100 154200 154300 154400 154500 154600 154700 154800 154900 155000 155100 155200 155300 155400 155500 155600 155700 155800 155900 156000 156100 156200 156300 156400 156500 156600 156700 156800 156900 157000 157100 157200 157300 157400 157500 157600 157700 157800 157900 158000 158100 158200 158300 158400 158500 158600 158700 158800 158900 159000 159100 159200 159300 159400 159500 159600 159700 159800 159900 160000 160100 160200 160300 160400 160500 160600 160700 160800 160900 161000 161100 161200 161300 161400 161500 161600 161700 161800 161900 162000 162100 162200 162300 162400 162500 162600 162700 162800 162900 163000 163100 163200 163300 163400 163500 163600 163700 163800 163900 164000 164100 164200 164300 164400 164500 164600 164700 164800 164900 165000 165100 165200 165300 165400 165500 165600 165700 165800 165900 166000 166100 166200 166300 166400 166500 166600 166700 166800 166900 167000 167100 167200 167300 167400 167500 167600 167700 167800 167900 168000 168100 168200 168300 168400 168500 168600 168700 168800 168900 169000 169100 169200 169300 169400 169500 169600 169700 169800 169900 170000 170100 170200 170300 170400 170500 170600 170700 170800 170900 171000 171100 171200 171300 171400 171500 171600 171700 171800 171900 172000 172100 172200 172300 172400 172500 172600 172700 172800 172900 173000 173100 173200 173300 173400 173500 173600 173700 173800 173900 174000 174100 174200 174300 174400 174500 174600 174700 174800 174900 175000 175100 175200 175300 175400 175500 175600 175700 175800 175900 176000 176100 176200 176300 176400 176500 176600 176700 176800 176900 177000 177100 177200 177300 177400 177500 177600 177700 177800 177900 178000 178100 178200 178300 178400 178500 178600 178700 178800 178900 179000 179100 179200 179300 179400 179500 179600 179700 179800 179900 180000 180100 180200 180300 180400 180500 180600 180700 180800 180900 181000 181100 181200 181300 181400 181500 181600 181700 181800 181900 182000 182100 182200 182300 182400 182500 182600 182700 182800 182900 183000 183100 183200 183300 183400 183500 183600 183700 183800 183900 1840

10/519263

WO 2004/006520

PCT/AU2003/000860

5/6

Screen Shot 5 - Telstra Big Pond Home Internet Explorer

Machine	Section	IP Address	Mac Address	Active			
Gaming 2	Game Machines	192.168.1.2	00:80:AD:06:97:B7	Yes	Save	Adv	Delete
Gaming 3	Game Machines	192.168.1.3	00:80:AD:85:E2:0C	Yes	Save	Adv	Delete
Gaming 4	Game Machines	192.168.1.4	00:80:AD:08:BB:B3	Yes	Save	Adv	Delete
Gaming 5	Game Machines	192.168.1.5	00:80:AD:7C:FD:FC	Yes	Save	Adv	Delete
Gaming 7	Game Machines	192.168.1.7	00:80:AD:85:E4:00	Yes	Save	Adv	Delete
Gaming 8	Game Machines	192.168.1.8	00:80:AD:85:DD:AC	Yes	Save	Adv	Delete
Gaming 8	Game Machines	192.168.1.9	00:80:AD:7D:05:E5	Yes	Save	Adv	Delete
Gaming 10	Game Machines	192.168.1.10	00:80:AD:08:BB:C8	Yes	Save	Adv	Delete
Gaming 11	Game Machines	192.168.1.11	00:80:AD:08:BB:A9	Yes	Save	Adv	Delete
Gaming 1	Game Machines	192.168.1.13	00:80:AD:71:4B:C1	Yes	Save	Adv	Delete
Auto_Conf	Game Machines	192.168.1.75	00:80:AD:7D:E1:4D	No	Save	Adv	Delete
Auto_Conf	Game Machines	192.168.1.160	00:80:AD:39:D2:7B	No	Save	Adv	Delete
Glen	Staff Machines	192.168.1.241	00:80:AD:74:76:F4	Yes	Save	Adv	Delete
Cust Entry	Staff Machines	192.168.1.251	00:80:AD:76:2C:09	Yes	Save	Adv	Delete
Jeff	Staff Machines	192.168.1.253	00:80:AD:73:B2:69	Yes	Save	Adv	Delete
Matt	Staff Machines	192.168.1.97	00:80:AD:72:FD:91	Yes	Save	Adv	Delete

FIG 5

10/519263

WO 2004/006520

PCT/AU2003/000860

6/6

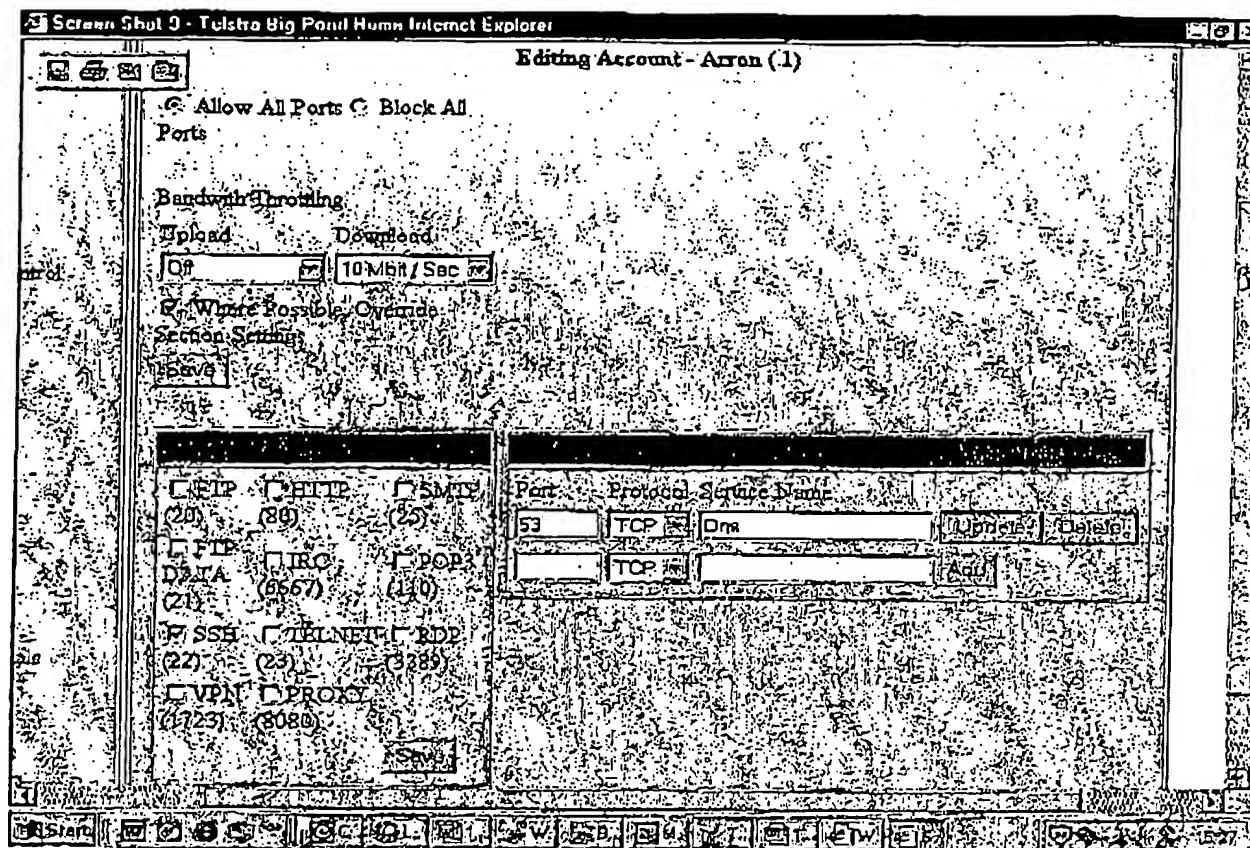


FIG 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/AU03/00860

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. ⁷: H04L 12/66, 29/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPAT, esp@cenet, USPTO; keywords (gateway, firewall, access, rules, modify, monitor)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 99/34544 A1 (UKIAH SOFTWARE, INC.) 8 July 1999 In particular page 21 - page 23 & figure 1	1-26
X	US 5867483 A (ENNIS, JR. ET AL.) 2 February 1999 See whole document	1-26
Y	US 6233618 B1 (SHANNON) 15 May 2001 See whole document	1, 8-18, 24, 26
Y	US 6052730 A (FELCIANO ET AL.) 18 April 2000 col 4 line 37 - col 5 line 42	1, 8-18, 24, 26
Note: For the Y indications, US 6233618 and US 6052730 may be combined for relevance to claims 1, 8-18, 24 & 26.		



Further documents are listed in the continuation of Box C



See patent family annex

* Special categories of cited documents:

"A" Document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" Document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" Document referring to an oral disclosure, use, exhibition or other means

"P" Document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
20 August 2003

Date of mailing of the international search report

9 SEP 2003

Name and mailing address of the ISA/AU

AUSTRALIAN PATENT OFFICE
PO BOX 200, WODEN ACT 2606, AUSTRALIA
E-mail address: pct@ipaustalia.gov.au
Facsimile No. (02) 6285 3929

Authorized officer

ROBERT BARTRAM

Telephone No : (02) 6283 2215

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/AU03/00860

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member			
WO 9934544		AU 23076/99	CA 2316355	EP 1050128	
		US 6578077	US 6502131	US 6047322	
		US 6119235	US 6137777	US 6292465	
		US 6341309	AU 58963/99	WO 200035130	
US 5867483		CA 2270890	EP 0976212	WO 199821845	
US 6233618		NONE			
US 6052730		NONE			
					END OF ANNEX

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.